

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 06-268777
 (43)Date of publication of application : 22.09.1994

(51)Int.Cl. H04M 15/00
 H04B 7/26
 H04L 9/00
 H04L 9/10
 H04L 9/12
 H04Q 7/04

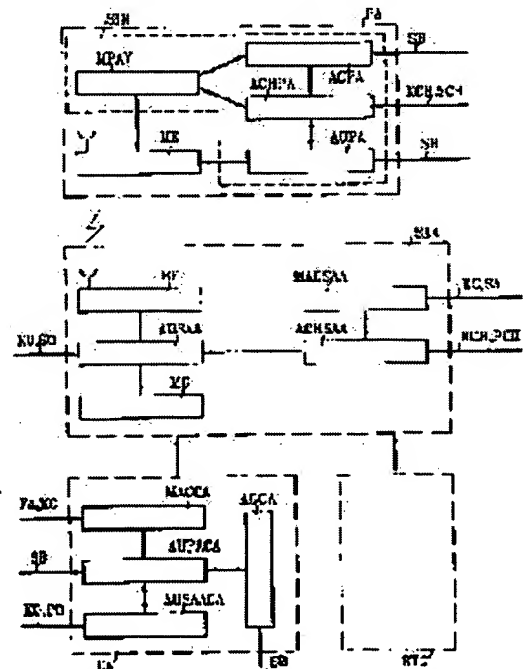
(21)Application number : 05-235086 (71)Applicant : FR TELECOM
 LA POSTE
 (22)Date of filing : 21.09.1993 (72)Inventor : NEVOUX ROLA
 HIOLE PHILIPPE

(30)Priority
 Priority number : 92 9211223 Priority date : 21.09.1992 Priority country : FR

(54) LONG-DISTANCE COMMUNICATION FACILITY HAVING PREPAYMENT MEANS TO BE SAFELY REMOTE LOADED AND REMOTE LOADING METHOD FOR THE FACILITY

(57)Abstract:

PURPOSE: To secure both secrecy and maintenance for a remote loading method of value unit for prepayment.
 CONSTITUTION: This facility includes an active authentication mode of an independent set (PA) and an access system (SAA), a calculation mode of a remote loading master key (KCH or (SCH, PCH)) set at the level of a certification center (CA), a transmission mode set to the access system (SAA) of an enciphered remote loading master key, and a remote loading mode that offers a safe remote loading method of a prepayment means (MPAY) to be executed by the access system with the help of the remote loading master key that is transmitted in the said way respectively in response to a prescribed number of remote loading request words (R) of value units which are given from the set (PA).



LEGAL STATUS

[Date of request for examination] 14.09.2000
 [Date of sending the examiner's decision of rejection]
 [Kind of final disposal of application other than the examiner's decision of rejection or

application converted registration]
[Date of final disposal for application]
[Patent number]
[Date of registration]
[Number of appeal against examiner's decision
of rejection]
[Date of requesting appeal against examiner's
decision of rejection]
[Date of extinction of right]

Copyright (C); 1998,2003 Japan Patent Office

(19) 日本国特許庁 (JP)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平6-268777

(43) 公開日 平成6年(1994)9月22日

(51) Int. Cl.⁵ 識別記号 庁内整理番号 FI 技術表示箇所

H04M 15/00

G 7190-5K

Z 7190-5K

H04B 7/26

109

S 7304-5K

H04L 9/00

9/10

審査請求 未請求 請求項の数15 OL (全16頁) 最終頁に続く

(21) 出願番号 特願平5-235086

(22) 出願日 平成5年(1993)9月21日

(31) 優先権主張番号 9211223

(32) 優先日 1992年9月21日

(33) 優先権主張国 フランス (FR)

(71) 出願人 591034154

フランス・テレコム

FRANCE TELECOM

フランス国、75015 パリ、プラス・ダ
ル、6

(71) 出願人 592132006

ラ・ポスト

LA POSTE

フランス国、75027 パリ・セデ、アベ
ニ・ド・セグール、20

(74) 代理人 弁理士 筒井 大和 (外2名)

最終頁に続く

(54) 【発明の名称】 安全に遠隔ローディングされる前払い手段を備えた遠距離通信設備およびその遠隔ローディング方法

(57) 【要約】

【目的】 前払い用の価値単位の遠隔ローディングの秘密性および保全性を確保する。

【構成】 本設備は、独立セット (PA) から発せられる所定の数の価値単位の遠隔ローディング要請ワード (R) に応じて：一独立セット (PA) およびアクセス・システム (SAA) の能動的な認証；一認可センター (CA) のレベルでの遠隔ローディング・マスターキー (KCHあるいは (SCH, PCH)) の計算；一暗号化された遠隔ローディング・マスターキーのアクセス・システム (SAA) へ向けた送信；一このように送信された遠隔ローディング・マスターキーの助けを得てアクセス・システムにより行なわれる前払い手段 (MPAY) の安全な遠隔ローディング、が提供される遠隔ローディング・モードを含む。

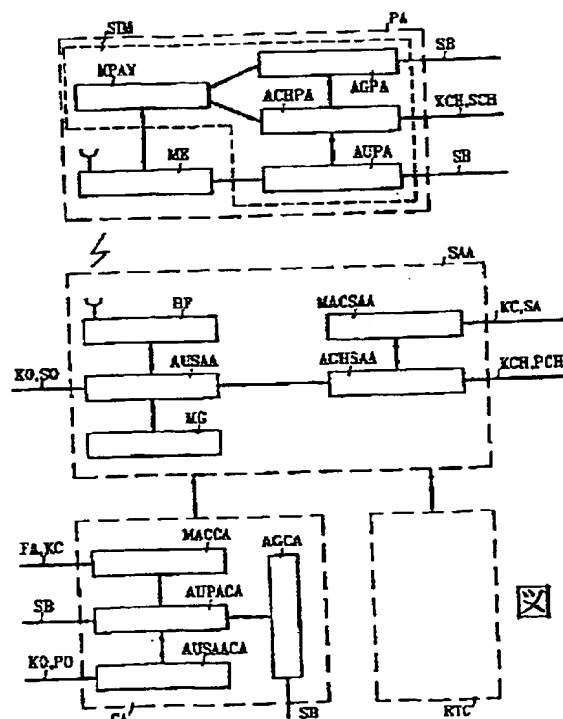


図 1

【特許請求の範囲】

【請求項1】 遠距離通信設備で、次のもの、すなわち：

一 少なくとも一つの交換電話ネットワーク (RTC) ；
 一 自立電話加入者アクセス・システム (SAA) で、次のもの、すなわち：

・ 前記交換電話ネットワークに連結された少なくとも一つのベース局 (BF) ；

・ 前記ベース局に接続され、前記交換電話ネットワーク (RTC) の有料サービスの利用に対する料金を計算することができる料金計測手段 (MG) を含む、操作手段；

・ 格納マスターキー (KCあるいはFA) の助けを得て暗号関数 (ACあるいはFC) を確立することができる第一の暗号化／復号手段 (MACSAA) ；

を有するアクセス・システム (SAA) ；

一 少なくとも一つの独立セット (PA) で、次のもの、すなわち：

・ 前記ベース局 (BF) と相互通信を確立することができる手段；

・ 前記料金計測手段により計算され送信される利用料金を支払うために用いられる価値単位を収容することができる前払い手段 (MPAY) ；

・ 各加入者に固有の所定のセット・ベース・マスターキー (SB) の助けを得て認証関数 (A) を確立することができる第一のセット認証手段 (AUPA) ；

を含む独立セット (PA) ；

一 認可センター (CA) であって、次のもの、すなわち：

・ 前記格納マスターキー (KCあるいはFA) の助けを得て暗号化／復号関数 (ACあるいはFC) を確立することができる第二の暗号化／復号手段 (MACCA) ；

・ 前記セット・ベース・マスターキー (SB) の助けを得てセット認証関数 (A) を確立することができる第二のセット認証手段 (AUPACA) ；

を有する認可センター (CA) ；

からなる遠距離通信設備であって、

前記独立セット (PA) が、更に：

一 前記セット・ベース・マスターキー (SB) の助けを得て生成関数 (AG) を確立することができる第一の生成手段 (AGPA) ；

一 前記セット・ベース・マスターキー (SB) の助けによって前記生成関数 (AG) による所定のワードの変換として得られた遠隔ローディング・マスターキー (KCHあるいはSCH) の助けを得て遠隔ローディング関数 (ACHあるいはSCH) を確立することができる第一の遠隔ローディング手段 (ACHPA) ；

を有し、

前記アクセス・システム (SAA) が、更に：

一 所定のシステム・ベース・マスターキー (KOあるいは

はSO) の助けを得てシステム認証関数 (AOあるいはFO) を確立することができる第二のシステム認証手段 (AUSAA) ；

一 所定の数の価値単位を発行することができ、また、前記遠隔ローディング・マスターキー (KCHあるいはPCH) の助けを得て遠隔ローディング関数 (ACHあるいはFCH) を確立することができる第二の遠隔ローディング手段 (ACHSAA) ；

を有し、

前記認可センター (CA) が、更に：

一 前記システム・ベース・マスターキー (KOあるいはPO) の助けを得てシステム認証関数 (AOあるいはFO) を確立することができる第二のシステム認証手段 (AUSAACA) ；そして、

一 前記セット・ベース・マスターキー (SB) の助けを得て生成関数 (AGあるいはFG) を確立することができる第二の生成手段 (AGCA) ；

を有し、

本遠距離通信設備が、更に、遠隔ローディング・モードを有し、該遠隔ローディング・モードにおいては、前記

独立セット (PA) から発せられる所定の数の価値単位に関する遠隔ローディング要請ワード (R) に応じて、

前記第一および第二のセット認証手段 (AUPAおよびAUPACA) ならびに前記第一および第二のシステム認証手段 (AUSAAおよびAUSAACA) が、それ

ぞれ前記アクセス・システムから発せられるセット認証ワード (RO) と、前記セット・ベース・マスターキー (SB) の助けを得て前記セット認証関数 (A) により

得られる該ワード (RO) の変換 (RESO) とを交換し、また、前記認可センター (CA) から発せられるシステム認証ワード (R2) と、前記システム・ベース・

マスターキー (KOあるいはSO) の助けを得て前記システム認証関数 (AOあるいはFO) により得られる該ワード (R2) の変換 (RES2) とを交換することにより、該独立セットおよび該アクセス・システムのそれ

ぞれの能動的認証を実行し、前記アクセス・システムおよび前記独立セットの認証がチェックされる場合、前記認可センター (CA) のレベルで前記第二の生成手段 (AGCA) が、前記セット・

ベース・マスターキー (SB) の助けを得て前記生成関数 (AG) により遠隔ローディング要請ワードの変換として得られる遠隔ローディング・マスターキー (KCH

あるいはSCH, PCH) を計算し、前記遠隔ローディング・マスターキーが前記認可センターで生成される場合、前記第二の暗号化／復号手段 (MACCA) が前記格納マスターキー (KCあるいはFA) の助けを得て暗号化されたローディング・マスター

キー (EKCHあるいはEPCH) を前記第一の暗号化／復号手段 (MACSAA) に送信し、該第一の暗号化／復号手段はアクセス・システム (SAA) のレベルで

／復号手段はアクセス・システム (SAA) のレベルで

格納するためにそれを復号し、

遠隔ローディング・マスターキーが該アクセス・システム(SAA)に格納される場合には、安全な方法で価値単位の数(n)を前払い手段に遠隔ロードする目的で、第一および第二の遠隔ローディング手段(ACHSAAおよびACHPA)が遠隔ロードされるべき価値単位の数(n)に対する遠隔ローディング要請ワード(R)、ならびに、遠隔ローディング・マスターキー(KCHあるいは(SCH, PCH))の助けを得てなされる該遠隔ローディング要請ワード(R)の遠隔ローディング関数(ACHあるいはFCH)による変換(RES)、を交換する、ものであることを特徴とする遠距離通信設備。

【請求項2】 前記遠隔ローディング要請ワード(R)およびその変換(RES)を交換する前に、遠隔ローディング依頼の認可を認証する目的で、第一および第二のシステム認証手段(AUSAAおよびAUSAACA)が、認可認証ワード(R1)および、システム認証マスターキー(KOあるいは(PO, SO))の助けを得てシステム認証関数(AOあるいはFO)により得られる該認可認証ワードの変換(RES1)を交換することを特徴とする請求項1の設備。

【請求項3】 前記遠隔ローディング要請ワード(R)およびその変換(RES)の交換と同時に、遠隔ローディング依頼の受信を認証する目的で、第一および第二の遠隔ローディング手段(ACHSAAおよびACHPA)が受信認証ワード(R2)、および、遠隔ローディング・マスターキー(KCHあるいは(PCH, SCH))の助けを得て遠隔ローディング関数(ACHあるいはFCH)によりなされる該受信認証ワード(R2)の変換(RES2)を交換することを特徴とする請求項1および2のいずれか1項の設備。

【請求項4】 前記セット認証関数(A)、前記システム認証関数(AO、FO)、前記暗号化/復号関数(AC、FC)、前記生成関数(AG)あるいは前記遠隔ローディング関数(ACHあるいはFCH)がDESあるいはRSAタイプの暗号アルゴリズムであることを特徴とする請求項1ないし3のいずれか1項の設備。

【請求項5】 前記前払い手段(MPAY)の遠隔ローディングの手続きが通信中にリアルタイムで生じること

を特徴とする請求項1ないし4のいずれか1項の設備。

【請求項6】 前記前払い手段(MPAY)の遠隔ローディングの手続きが、呼び出しが確立する前に、加入者の要請であるいはネットワークの主導で生じること

を特徴とする請求項1ないし4のいずれか1項の設備。

【請求項7】 前記前払い手段(MPAY)、第一の遠隔ローディング手段(ACHPA)、第一の生成手段(AGPA)および第一のセット認証手段(AUPA)が、無線相互通信を確立するための手段(ME)と協働することができる着脱可能な加入者識別モジュール(S

IM)に収納されていることを特徴とする請求項1ないし6のいずれか1項の設備。

【請求項8】 前記加入者識別モジュールが、外界からのふさわしくない時期になされるデータの書き込みに対して保護されてまた価値単位を収容することができるメモリ、および該価値単位の助けにより利用料金を支払い、また遠隔ロードされた価値単位の助けによりメモリを再ロードすることができる処理装置を有していることを特徴とする請求項1ないし7のいずれか1項の設備。

【請求項9】 前記加入者識別モジュール(SIM)が標準的なISOタイプのカードに収容され、前記無線相互通信を確立するための手段(ME)が該カードを読み取るための読み取り装置を有していることを特徴とする請求項1ないし8のいずれか1項の設備。

【請求項10】 前記加入者識別モジュールが、前記無線相互通信を確立するための手段(ME)に差し込むことができる機械的なインタフェースを有していることを特徴とする請求項1ないし8のいずれか1項の設備。

【請求項11】 前記独立セットおよび前記ベース局との間の相互通信が無線あるいは有線によりなされることを特徴とする請求項1ないし10のいずれか1項の設備。

【請求項12】 前記独立セットが移動可能あるいは固定式で、個人用あるいは公衆用のものであることを特徴とする請求項1ないし11のいずれか1項の設備。

【請求項13】 前払い手段の安全な遠隔ローディングのための方法であって、次のステップ、すなわち：

— a) 少なくとも一つの交換電話ネットワーク(RTC)を提供し；

— b) 自立的な電話加入者アクセス・システム(SAA)であって、次のもの、すなわち：

・ b1) 前記交換電話ネットワークに連結された少なくとも一つのベース局(BF)

・ b2) 該ベース局に連結された操作手段であって、前記交換電話ネットワーク(RTC)の有料サービスの利用に対する料金を計算することができる料金計測手段(MG)を有する、操作手段、

を有するアクセス・システム(SAA)を提供し；

— c) 少なくとも一つの独立セット(PA)であって、次のもの、すなわち：

・ c1) 前記ベース局(BF)との相互通信を確立することのできる手段；

・ c2) 前記料金計測手段により計算され送信される利用料金を支払うための価値単位を収容することができる前払い手段(MPAY)；

・ c3) 各加入者に固有な所定のセット・ベース・マスターキー(SB)の助けにより認証関数(A)を確立することができる第一のセット認証手段(AUPA)；

を有する少なくとも一つの独立セット(PA)を提供し；

- d) 認可センター (CA) であって、次のもの、すなわち:

・ d 1) 格納マスターキー (KCあるいはFA) の助けにより暗号化/復号関数 (ACあるいはFC) を確立することができる第二の暗号化/復号手段 (MACCA) ;

・ d 2) セット・ベース・マスターキー (SB) の助けによりセット認証関数 (A) を確立することができる第二のセット認証手段 (AUPACA) ;

を有する認可センター (CA) を提供する ;
ステップからなる方法であって、

前記独立セット (PA) に対し次の備え、すなわち:

- 前記セット・ベース・マスターキー (SB) の助けにより生成関数 (AG) を確立することができる第一の生成手段 (AGPA) ;そして、- 前記セット・ベース・マスターキー (SB) の助けにより前記生成関数 (AG) により所定のワードの変換として得られる遠隔ローディング・マスターキー (KCHあるいはSCH) の助けにより、遠隔ローディング関数 (ACHあるいはFCH) を確立することができる第一の遠隔ローディング手
段 (ACHPA) ;

の備えが更に提供され ;

前記アクセス・システム (SAA) に対し次の備え、すなわち:

- 所定のシステム・ベース・マスターキー (KOあるいはSO) の助けによりシステム認証関数 (AOあるいはFO) を確立することができる第一のシステム認証手段 (AUSAA) ;そして

- 所定の数の価値単位を発行することができ、また、遠隔ローディング・マスターキー (KCHあるいはPCH) の助けにより遠隔ローディング関数 (ACHあるいはSCH) を確立することができる第二の遠隔ローディング手段 (ACHSAA) ;

の備えが更に提供され ;

前記認可センター (CA) に対し次の備え、すなわち:

- 前記システム・ベース・マスターキー (KOあるいはPO) の助けによりシステム認証関数 (AOあるいはFO) を確立することができる第二のシステム認証手段 (AUSAACA) ;そして

- 前記セット・ベース・マスターキー (SB) の助けにより生成関数 (AG) を確立することができる第二の生成手段 (AGCA) ;

の備えが更に提供され ; 本方法が、更に、遠隔ローディング・ステップを含み、該ステップにおいては、前記独立セット (PA) から発せられる所定の数の価値単位に関する遠隔ローディング要請ワード (R) に応じて、第一および第二のセット認証手段 (AUPAおよびAUPACA) ならびに第一および第二のシステム認証手段 (AUSAAおよびAUSAACA) が、それぞれ前記アクセス・システムから発生されるセット認証ワード

(RO) と、セット・ベース・マスターキー (SB) の助けを得てなされる該セット認証ワードのセット認証関

数 (A) による変換 (RES0) とを交換し、また、前記認可センター (CA) から発せられるシステム認証ワード (R2) と、システム・ベース・マスターキー (KOあるいはSO) の助けを得てなされる該システム認証

ワード (R2) のシステム認証関数 (AOあるいはFO) による変換 (RES2) とを交換することにより、

前記独立セットおよび前記アクセス・システムのそれぞれの能動的認証を実行し ; アクセス・システムおよび独立セットの認証がチェックされる場合、第二の生成手段 (AGCA) が認可センター (CA) のレベルで、セット・ベース・マスターキーの助けを得てなされる遠隔ローディング要請ワードの生成関数 (AG) による変換である遠隔ローディング・マスターキー (KCHあるいはSCH, PCH) を計算し ; 遠隔ローディング・マスターキーが前記認可センターのレベルで生成される場合には、第二の暗号化/復号手段 (MACCA) が、格納マスターキー (KCあるいはFA) の助けを得て暗号化されたローディング/マスターキー (EKCHあるいはEPCH) を第一の暗号化/復号手段 (MACSA) に送信し、該第一の暗号化/復号手段 (MACSA) はアクセス・システム (SAA) のレベルで格納する目的でそれを復号し ; 遠隔ローディング・マスターキーをアクセス・システム (SAA) に格納する場合には、第一および第二の遠隔ローディング手段 (ACHSAAおよびACHPA) が、安全な方法で価値単位の数 (n) を遠隔ローディングする目的で、遠隔ロードされるべき価値単位の数 (n) に対する遠隔ローディング要請ワード (R) 、および、遠隔ローディング・マスターキー (KCHあるいはPCH, SCH) の助けを得てなされる該遠隔ローディング要請ワードの遠隔ローディング関数 (ACHあるいはFCH) による変換 (RES) 、を交換する ; ことを特徴とする、前記手段の安全な遠隔ローディングのための方法。

【請求項14】 前記遠隔ローディング要請ワード

(R) およびその変換 (RES) を交換する前に、遠隔ローディング依頼の認可を認証する目的で、第一および第二のシステム認証手段 (AUSAAおよびAUSAACA) が認可認証ワード (R1) 、およびシステム認証マスターキー (KOあるいはSO, PO) の助けを得てシステム認証関数 (AOあるいはFO) により得られる該認可認証ワードの変換 (RES1) を交換することを特徴とする請求項13の方法。

【請求項15】 前記遠隔ローディング要請ワード

(R) およびその変換 (RES) を交換すると同時に、前記遠隔ローディング依頼の受信の認証を目的として、第一および第二の遠隔ローディング手段 (ACHSAAおよびACHPA) が受信認証ワード (R2) 、および、遠隔ローディング・マスターキー (KCHあるいは

(PCH, SCH)) の助けを得て遠隔ローディング関数 (ACH あるいは FCH) によりなされる該受信認証ワード (R2) の変換 (RES2) を交換することの特徴とする請求項 13 および 14 のいずれか 1 項の方法。

【発明の詳細な説明】

【0001】

【産業上の利用分野】本発明は、前払い手段の安全な遠隔充填 (ローディング) に関するものである。

【0002】本発明は遠距離通信に一般的に適用でき、特に、「移動通信のための広域システム (GSM, GLOBAL SYSTEM FOR MOBILE COMMUNICATION) 」と呼ばれる、900Hz で運営される公衆車両との通信のためのデジタル・システムに適用できる。

【0003】

【従来の技術】知られているように、遠距離通信の設備は次のものを含んでいる：

- 一 少なくとも一つの交換電話ネットワーク；
- 一 次のものを含む独立電話加入者アクセス・システム；
- ・ 前記交換電話ネットワークに連結された少なくとも一つのベース局 (基地局) ；
- ・ 前記ベース局に連結された操作手段であって、前記交換電話ネットワークの有料サービスの利用に対する料金を計算することのできる料金計測手段を含む、操作手段；
- ・ 格納マスターキーの助けを得て暗号関数を実現することのできる第一の暗号化／復号手段；
- 一 次のものを含む少なくとも一つの独立セット (独立通信機) ；
- ・ 前記ベース局との相互通信を確立できる手段；
- ・ 前記料金計測手段により計算され送信される利用料金の支払いにあてるための価値単位を収容する前払い手段；
- ・ 各加入者に固有な所定のセット・ベース・マスターキーの助けを得てセット認証関数を実現することのできる第一のセット認証手段；
- 一 次のものを含む認可センター；
- ・ 前記格納マスターキーの助けを得て暗号化／復号関数を実現できる第二の暗号化／復号手段；
- ・ 前記セット・ベース・マスターキーの助けを得てセット認証関数を実現できる第二のセット認証手段。

【0004】

【発明が解決しようとする課題】例えば、無線電話への応用の場合、独立セットは、第一および第二のセット認証手段を用いて独立セットに関する加入者の識別を認証するための操作が完了した後、交換電話ネットワークの有料サービスにアクセスする。

【0005】独立セットに対する加入者の識別認証が、独立セットと認可センター間で、ランダム数、および、各加入者の固有のセット・ベース・マスターキーの助けを得たセット認証関数によるこのランダム数の変換、を

交換する能動的な認証であるのは好ましい。

【0006】しかし、このような認証は、加入者を認証

し、この加入者が交換電話ネットワークの有料サービスにアクセスするのを認可することができるだけである。

【0007】それは、このように識別されアクセスが認可された加入者と「会話」する設備に関して、利用料金の支払いに役立つ前払い手段が通信の継続中、すべてを包括しているという保証を可能にすることはない。

【0008】本出願人による1990年10月10日付けのフランス国特許出願第9012510号は、第一および第二のセット認証手段の助けを得て、通信の継続中利用料金の能動的認証を用いることにより、この問題に対する解決を提供した。

【0009】この利用料金の能動的な認証は特に次のことを可能にする：

- 一 料金計測手段により無線電話インタフェースを介して前払い手段へ送信された利用料金の証明；
- 一 それらの利用料金が正しく受信され理解されたことの実証；
- 一 それらが実際に前払い手段から差し引かれたことの実証。

【0010】更に、前払い手段の勘定に所定の数の価値単位を再ロードするための手続きが知られている。

【0011】これらの手続きは、一般的に通信それ自体の外部で、ローカルに、例えば、認可センターで直接に、あるいは認可センターと何の連結もない「オフライン」の独立セットにおいて、あるいは遠隔的に、例えば、ミニテル (MINITEL 、商標) サーバーによる遠隔ローディングのような特定のアプリケーションを介して、発生する。しかし、後者の手続きの場合、遠隔ロードされた量の適切な受信の保証や、独立セットによるその遠隔ローディングが拒絶されないという保証がない。

【0012】更に、前払い手段の遠隔ローディングは、前払い手段を発行しあるいは管理する認可センターとは異なる、そして独立セットが商業的に所属しない、第三者の認可センターにより加入者がチェックされる時に必要とされるかもしれない (これは、例えば、加入者が自分の独立セットをその管理に責任を持つ運営者とは異なる運営者によりカバーされる区域において利用する場合、つまり、GSMアプリケーションにおけるいわゆる「ぶらつき (ROAMING) 」サービスの場合がそうである。

【0013】この状況において、第三者の認可センターの側の主導で行なう前払い手段の遠隔ローディングという解決策は安全性の点で満足すべきものではない。

【0014】実際、遠隔ローディング依頼およびその量に関する秘密性および保全性は保証されないので、欺瞞的な再生が可能かもしれない。

【0015】本発明はこの問題に対する解決を提供する。

【0016】それで、本発明の目的は、独立セットが商業的に所属しないアクセス・システム(GSMアプリケーションではいわゆる「ぶらつき」サービス)に加入者がアクセスする場合でも、遠隔ローディングの依頼およびその量の秘密性および安全性を確保することのできる遠距離通信設備を提供することである。

【0017】本発明の目的は、また、このようにアクセスされるアクセス・システムに関して、遠隔ローディングの依頼およびその量が正しく受信され理解されたこと、そして前払い手段の単位メーターがこのように遠隔ロードされた価値単位の数を実際に再ロードされたことを保証することである。

【0018】本発明の目的は、最後に、加入者による遠隔ローディング依頼が拒絶されないことを保証する前払い手段の安全な遠隔ローディングの方法を提供することである。

【0019】

【課題を解決するための手段】本発明は上述のタイプの遠距離通信設備からスタートする。

【0020】本発明の最初の特徴によれば、独立セットは更に次のものを有している：

—セット・ベース・マスターキーの助けを得て生成関数を確立することができる第一の生成手段；
—セット・ベース・マスターキーの助けを得て生成関数による所定のワードの変換である遠隔ローディング・マスターキーの助けを得て遠隔ローディング関数を確立できる第一の遠隔ローディング手段。

【0021】アクセス・システムは更に次のものを有している：

—所定の遠隔ローディング依頼に応じて所定の数の価値単位を発行でき、また遠隔ローディング・マスターキーの助けを得て遠隔ローディング関数を確立することができる第二の遠隔ローディング手段；
—所定のシステム・ベース・マスターキーの助けを得てシステム認証関数を確立することができる第一のシステム認証手段。

【0022】認可センターは更に次のものを有している：

—システム・ベース・マスターキーの助けを得てシステム認証関数を確立できる第二のシステム認証手段；そして、
—セット・ベース・マスターキーの助けを得て生成関数を確立できる第二の生成手段。

【0023】本発明の設備は、更に、遠隔ローディング・モードを含んでおり、そのモードにおいては、独立セットから発せられる所定の数の価値単位に対する遠隔ローディング要請ワードに応じて、第一および第二のセット認証手段および第一および第二のシステム認証手段は、独立セットから発せられるセット認証ワードと、セット・ベース・マスターキーの助けを得てセット認証関

数により得られるこのワードの変換とをそれぞれ交換することにより、また、認可センターから発せられるシステム認証ワードと、システム・ベース・マスターキーの助けを得てシステム認証関数により得られるこのシステム認証ワードの変換を交換することにより、独立セットおよびアクセス・システムのそれぞれの能動的な認証を実行する。

【0024】アクセス・システムおよび独立セットの認証がチェックされる場合、第二の生成手段は、認可センターのレベルで、遠隔ローディング要請ワードの変換(セット・ベース・マスターキーの助けを得て生成関数により得られる)である遠隔ローディング・マスターキーを計算する。

【0025】認可センターのレベルでの遠隔ローディング・マスターキーの生成の場合、第二の暗号化/復号手段が暗号化されたローディング・マスターキーを格納マスターキーの助けを得て第一の暗号化/復号手段に送信し、第一の暗号化/復号手段は、アクセス・システムのレベルで格納することを目的としてそれを復号する。

【0026】遠隔ローディング・マスターキーがアクセス・システムに格納される場合には、安全な方法で価値単位の数を前払い手段に遠隔ロードする目的で、第一および第二の遠隔ローディング手段が遠隔ロードされるべき価値単位の数に関する遠隔ローディング要請ワード、ならびに、遠隔ローディング・マスターキーの助けにより得られる該遠隔ローディング要請ワードの遠隔ローディング関数による変換を交換する。

【0027】このような設備は、第一の操作者により前払い手段が引き渡された加入者で、第二の操作者によりチェックされながら「動き回る」加入者が任意の時点で自分の前払い手段に遠隔ロードすることを可能にするので有利である。更に、遠隔ローディングは動的に、安全にそして適切なら通信を中断することなく行なえる。

【0028】所定の数の価値単位の遠隔ローディングに対する要請が電話通信の外部において、加入者の要請により行なわれれば有利である。

【0029】変形として、所定の数の価値単位の遠隔ローディングの要請が電話通信の際に行なわれるようにすることもできる。

【0030】本発明はまた、上述のタイプの遠隔ローディング・モードに依存する前払い手段の安全な遠隔ローディングのための方法に関するものである。

【0031】本発明の他の特徴および有利な点は以下の説明ならびに添付図面から明らかにされるであろう。

【0032】

【実施例】図1において、既知のタイプの無線電話設備は、移動可能な独立電話加入者アクセス・システムSAAを、複数の移動あるいは固定独立セットPAと協働するように配置している。

【0033】アクセス・システムSAAは複数のベース

局BFを含み、ベース局の各々は交換電話ネットワークRTCに連結されている。

【0034】本発明の理解を容易にするために、図1では独立セットPAおよびベース局BFがそれぞれ一つずつしか示されていない。

【0035】各独立セットPAは最も近いベース局BFと無線電話による相互通信を確立するための手段MEを有している。

【0036】アクセス・システムSAAに接続された認可センターCAは、後でより詳細に説明するが、アクセス・システムと独立セットとの間の通信を監督しチェックする。

【0037】この種の設備は、例えばGSMに適用されているが、L'ECHO DES RECHERCHES誌、No. 131、1988年、第一季号、5-16ページ、B. GHILLEBERT, P. COMBESURE, A. MALOBERTI の記事、および同じ雑誌の No. 139、1990年、第一季号、13-19ページ、P. JOLIE, G. MAZZIOTTO の記事に説明されている。

【0038】実際的には、アクセス・システムのレベルでは、ベース局BFに連結された操作手段が設けられており、この操作手段は交換電話ネットワークRTCの有料サービスの利用に対する料金を計算できる料金計測手段MGを有している。

【0039】独立セットPAの側では、前払い手段MPAYを有しており、この前払い手段MPAYは遠隔的に再ロードすることができ、処理装置（図示されていない）およびメモリ（図示されていない）を備え、メモリは料金計測手段により計算され送信される利用料金の支払いにあてるための価値単位を収納することができる。

【0040】実際的には、メモリは外界からのふさわしくない時期になされるデータの直接書き込みに対し保護されている。

【0041】GSMへ適用する場合、前払い手段MPAYが、独立セットPAの無線相互通信を確立するための手段MEと協働する着脱可能な加入者識別モジュールSIMに収納されているのは有利である。

【0042】前払い手段MPAYのメモリがEPROMあるいはEEPROMタイプのもので、SIMモジュールの処理装置により正しく保護されているのは好ましい。

【0043】SIMモジュールは標準的なISOタイプのカードに収納されている。

【0044】変形として、SIMモジュールを無線相互通信を確立するための手段MEにプラグで差し込まれるコンポーネントとすることもできる。

【0045】フランス国特許出願第9012510号に記載されているように、独立セットのレベルでは、所定のセット・ベース・マスターキーSBの助けを得てセット認証関数Aを確立することができる第一のセット認証

手段AUPAが設けられており、認可センターCAのレベルでは、前記セット・ベース・マスターキーSBの助けを得てセット認証関数Aを確立できる第二のセット認証手段AUPACAが設けられている。

【0046】前記特許出願においては、第一および第二のセット認証手段AUPAおよびAUPACAは相互通信の間、利用料金の認証のために役立つことに注目すべきである。

【0047】GSMへの適用においては、セット・ベース・マスターキーSBは、例えば、各加入者に固有で例えば128ビット長の秘密マスターキーである。

【0048】セット認証関数Aに関して言えば、それは例えばDES (DATA ENCRYPTION STANDARD) タイプの暗号関数である。

【0049】既知のように、アクセス・システムSAAは、また、第一の暗号化/復号手段MACSAAが設けられており、それにより、格納マスターキーKCあるいはFAの助けにより暗号関数ACあるいはFCが確立される。

【0050】上述のように、本発明の目的は前払い手段の遠隔ローディングのための安全な手続きを提供することである。

【0051】この目的を達成するために、本発明の設備は、独立セットPAのレベルでは、セット・ベース・マスターキーSBの助けを得て生成関数AGを確立できる第一の生成手段AGPA、および、遠隔ローディングマスターキーKCHあるいはPCH（これはセット・ベース・マスターキーSBの助けを得た生成関数AGの変換である）の助けを得て遠隔ローディング関数ACHあるいはFCHを確立できる第一の遠隔ローディング手段ACHPAを備えることにより完成される。

【0052】つりあいとして、アクセス・システムSAAのレベルでは、本設備は、所定の数の価値単位nを発行し、遠隔ローディングマスターキーKCHあるいはPCHの助けを得て遠隔ローディング関数ACHを確立できる第二の遠隔ローディング手段ACHSAA、および、所定のシステム・ベース・マスターキーKOあるいはSOの助けを得てシステム認証関数AOあるいはFOを確立できる第一のシステム認証関数AUSAAを備えることにより完成される。

【0053】同じく、つりあひ上、認可センターCAは、本発明により、更に、セット・ベース・マスターキーSBの助けにより生成関数AGを確立できる第二の生成手段AGCGおよび、システム・ベース・マスターキーKOあるいはPOの助けを得てシステム認証関数AOあるいはFOを確立できる第二の認証手段AUSAAC Aを有している。

【0054】實際上、システム認証関数AOあるいはFO、セット認証関数A、暗号関数ACあるいはFC、遠隔ローディング関数ACHあるいはFCH、そして生成

関数AGは、「DES」(DATA ENCRYPTION STANDARD)あるいは「RSA」(RIVESTSHAMIR-ADELMAN)などの

暗号アルゴリズムに依存している。

【0055】これらDESあるいはRSAアルゴリズムは読み出し専用メモリに格納される。

【0056】DES暗号アルゴリズムは秘密ベース・マスターキーにより運営されることを思い起こすべきである。同様に、本設備の要素がDESの助けで会話できるためには、秘密マスターキーが会話する両方の要素に同時に格納されていなければならない。

【0057】これとは対照的に、RSAアルゴリズムは、実際には二つの互いに依存するマスターキー（すなわち、一つは二つの会話する要素のうちの一つに格納される公開マスターキー、もう一つは二つの要素の他の一つに格納される秘密マスターキー）の組合せであるベース・マスターキーの助けで運営される。

【0058】例えば、システム認証関数AOがDESアルゴリズムに依存する場合、秘密システム・ベース・マスターキーKOがシステムSAAのレベルで認証手段AUSAAに格納されると共に、認可センターCAのレベルで認証手段AUSACAに格納される。

【0059】このように、システム・ベース・マスターキーKOの助けを得たシステム認証関数AOによるランダム数Sの変換RESSは次のように書ける：

$$RESS = AO(KO, S)$$

これとは対照的に、システム認証関数FOがRSAアルゴリズムに依存する場合には、秘密システム・ベース・マスターキーSOはアクセス・システムAUSAAレベルでのみ格納され、公開システム・ベース・マスターキーPOは認可センターCAレベルで格納される。このように、秘密マスターキーSOの助けを得たシステム認証関数FOによるランダム数Sの変換RESSは次のように書ける：

$$RESS = SO(S)$$

他方、認可センターレベルで、システム認証手段AUSACAは、公開システム・ベース・マスターキーPOの助けを得て、システム認証関数FOによりワードRESSの変換を計算する。

【0060】アクセス・システムSAAの認証の立証は次のように書くことができる：

$$PO(RESS) = ?(S)$$

上の各式は、以下になされる本発明の遠隔ローディング手続きの詳細な説明において役に立つ。

【0061】RSAあるいはDES暗号アルゴリズムは商業的に市場で流通しているアルゴリズムである。

【0062】本発明の安全遠隔ローディング手続きは二つの部分に分かれる。

【0063】第一部分はアクセスされるアクセス・システムと前払い手段を管理する責任を負う認可センターとの間の交渉ステップからなっている。

【0064】簡単に言えば、それは独立セット、および認可センターとの関係におけるアクセス・システムの認

証が関係している。独立セットおよびアクセス・システムの認証がチェックされれば、認可センターはアクセス・システムに一時的遠隔ローディング・マスターキーを提供し、それによりアクセス・システムは前払い手段との関係で自分自身の認証が可能とする。

【0065】第二部分は、次に、遠隔的にそして安全に所定の数の価値単位をロードするために、アクセス・システムと前払い手段との間で生じる。

【0066】以下、図2および図3を参照して、本発明による遠隔ローディング手続きの第一部分を詳細に説明する。

【0067】實際上、前払い手段MPAYのために、アクセスされるアクセス・システムSAAは、相互通信の間、利用できるクレジット（利用できる単位数および使用される貨幣単位）を利用する。

【0068】例えば、この値があるしきい値に到達あるいは超えた場合（ステップ10）、アクセス・システムはセット認証ワードR0を生成し（ステップ12）、このセット認証ワードR0を独立セットに送る。

【0069】このセット認証ワードR0に応じて、独立セットは幾つかの解決に直面する。

【0070】まず第一に、前払い手段がアクセス・システムに属する場合。この場合、アクセス・システムがその前払い手段に遠隔ロードするために必要な情報を所有している。

【0071】第二に、アクセス・システムが認められている認可センターに前払い手段が属する場合。そのアクセス・システムは、それゆえ、前払い手段の遠隔ローディングのために必要な情報を所有する。

【0072】第三に、認可センターが認定していないアクセス・システムがアクセスされ、その認可センターに前払い手段が属する場合。アクセスされるそのアクセス・システムは、遠隔ローディングに必要な情報を得るために前払い手段の発行当局に接触しなければならない。

【0073】本発明による遠隔ローディング手続きが関係しているのは、この第三の状況であり、次のものを設定する必要がある：

40 ーアクセス・システムと認可センターの間の相互の認証のメカニズム；ー交換される秘密情報の秘密保護に関するメカニズム；そして、ー拒絶しないためのメカニズム。

【0074】このように、頻繁にやりとりのあるアクセス・システムが認められていない当局に前払い手段が属し、独立セットが前払い手段のクレジットのレベルにおいてしきい値を超過したことを通知される場合、前払い手段はn価値単位の遠隔ローディングの要請（これは遠隔ローディング要請ワードRとも呼ばれるランダム数を生成することである）を行ない、このランダム・ワード

Rをアクセス・システムSAAに送り返す。

【0075】次に、ステップ16において、第一のセット認証手段は、セット・ベース・マスターキーSBの助けを得てセット認証関数Aによりセット認証ワードR0の変換RES0を計算する。この変換RES0の計算には要請された価値単位の数nも関与している。

【0076】ステップ16が完了すると、遠隔ローディング要請ワードR、変換RES0および価値単位の数nがアクセス・システムSAAに送られる。これらのワードR、RES0およびnに応じて、アクセス・システムはクレジット認証要請を行なう（ステップ18）。このクレジット認証要請とは、クレジット認証要請ワードR1を生成し、ワードR1、R、R0、RES0およびnを認可センターCAに送る（ステップ20）ことである。

【0077】これらのワードに応じて、認可センターはシステム認証要請を行なう（ステップ22）。これは、システム認証ワードR2を生成し、このシステム認証ワードR2をアクセス・システムSAAに送ることである。アクセス・システムおよび認可センターの相互の認証は第一および第二のシステム認証手段AUSAAおよびAUSACAにより担われる（ステップ22、24、26）。

【0078】ステップ24において、システム認証関数はDESタイプの暗号アルゴリズムに依存するものとしてすることができる。その場合、ステップ24は秘密システム・ベース・マスターキーKOの助けを得て認証関数AOによりワードR2の変換RES2を計算する。

【0079】これとは対照的に、システム認証手段がRSAタイプの暗号アルゴリズムに依存する場合、システム認証手段は、システムSAAレベルで格納されている秘密マスターキーSOの助けを得て、システム認証ワードR2の変換RES2を計算する。

【0080】ステップ24で、価値単位の数nが変換RES2の計算に関与していることに注目すべきである。

【0081】最後に、ステップ24が完了すると、アクセス・システムSAAは変換RES2を認可センターに送る。

【0082】認可センターCAのレベルで、セットPAの認証およびシステムSAAの認証がチェックされる。

【0083】セットの認証のチェックについては、セット・ベース・マスターキーSBの助けを得て、セット認証関数AによりRES0'が計算（ステップ26）され、また、このように計算された変換RES0'と受け取られた変換RES0との比較が行なわれる。

【0084】システム認証のチェックに関しては、マスターキーKOの助けによりシステム認証関数AOによりRES2'が計算され（ステップ28）、また、このように計算された変換RES2'と受け取られた変換RES2との比較が行なわれる。ステップ28は、システム

認証手段がDESタイプのアルゴリズムに基づいている場合について示されている。

【0085】これとは対照的に、システム認証手段がRSAアルゴリズムに依存している場合には、ステップ30において、システムワードR2の認証の立証のために、認可センターレベルで格納されている公開マスターキーPOにより変換RES2の解読の計算が行なわれる。

【0086】独立セットおよびシステムの認証が立証されると、遠隔ローディング・マスターキーの計算が行なわれる（ステップ40）。遠隔ローディング・マスターキーがDESタイプのアルゴリズム秘密マスターキーである場合には、遠隔ローディング・マスターキーKCHは、マスターキーSBの助けを得て生成された関数AGによるクレジット要請ワードRの変換である（ステップ42）。

【0087】対照的に、RSAタイプのアルゴリズムの場合は、マスターキーSBの助けを得て生成するための関数AGにより、公開マスターキーPCHおよび秘密マスターキーSCHからなるマスターキーの組（PCH、SCH）を得ることができる（ステップ44）。公開マスターキーPCHはアクセス・システムSAAのレベルで格納される。

【0088】遠隔ローディング・マスターキーKCHあるいはPCHが認可センターレベルで生成されると、この遠隔ローディング・マスターキーKCHあるいは適切な場合にはこの遠隔ローディングマスターキーの公開部分PCHを暗号化してアクセス・システムに送信するのは適切である。

【0089】遠隔ローディング・マスターキーKCHあるいはPCHの暗号化はDESタイプの暗号アルゴリズムあるいはRSAタイプの暗号アルゴリズムの助けにより実行できる。

【0090】DESタイプの暗号アルゴリズムの場合には、認可センターCAレベルおよびアクセス・システムSAAレベルで格納マスターキーを利用するのは適切である。

【0091】例えば、格納マスターキーKCは、システム・ベース・マスターキーKOの助けによる暗号関数AGCによるワードR1の変換である（ステップ46および47）。

【0092】次いで、遠隔ローディング・マスターキーKCHの暗号化EKCH（ステップ48）が、アクセス・システムSAAおよび認可センターCAのレベルで利用できる秘密格納マスターキーKCの助けにより暗号関数ACにより実行される。

【0093】変形として、遠隔ローディング・マスターキーPCHの暗号化は、秘密格納マスターキーKCの助けを得て、暗号化関数ACにより実行される。

【0094】対照的に、RSAタイプの暗号化／復号ア

ルゴリズムの場合には、認可センターCAのレベルで公開マスターキーFA、アクセス・システムSAAのレベルで秘密マスターキーを利用するのが適切である。

【0095】遠隔ローディング・マスターキーKCHの暗号化EKCH（ステップ50）が次いで公開マスターキーFAの助けで実行される。

【0096】変形として、次いで、遠隔ローディング・マスターキーPCHの暗号化EPCHが、公開マスターキーFAの助けで実行される。

【0097】暗号化が行なわれると、マスターキーEKCHあるいはEPCH（ステップ52）がアクセス・システムSAAに送られ、アクセス・システムの側ではこのように暗号化されて受け取ったマスターキーを解読する。

【0098】暗号化／復号手段が適切に配置された当然の帰結として、マスターキーKCHあるいはPCHの復号が、ステップ54、56、58、60に記載された式に従って適切になされる。

【0099】次に、前払い手段の遠隔ローディングの第二部分に関して図4を参照する。

【0100】遠隔ローディングは、前払い手段の遠隔ローディングに責任を負うアクセス・システムSAAの料金計測手段と独立セットPAとの間で発生する。

【0101】先に詳細に述べたように、アクセス・システムSAAは遠隔ローディング関数ACHならびに一時的遠隔ローディング・マスターキーKCHあるいはPCHを利用する。

【0102】独立セットおよびアクセス・システムの認証、マスターキーKCHあるいは（PCH、SCH）の生成、その暗号化とアクセス・システムへの送信、およびそのマスターキーの暗号化が完了すると、最後に前払い手段の遠隔ローディングの手続が実施される。

【0103】独立セットもまた本質的に遠隔ローディング・マスターキーKCHあるいは（PCH、SCH）を利用することに注意されたい（ステップ100、102）。

【0104】アクセス・システムSAAは要請された価値単位の数nの関数として遠隔ロードされる量C1を確立する（ステップ104）。

【0105】アクセス・システムは、マスターキーKCHあるいは公開マスターキーPCHの助けを得て遠隔ローディング関数ACHを用いて、量C1に依存して、遠隔ローディング要請Rの変換RESを計算する（ステップ106）。

【0106】遠隔ローディング関数ACHはRSAタイプのアルゴリズム（PCH、SCH）あるいはDESタイプのアルゴリズム（秘密マスターキーKCH）に依存することに注意すべきである。

【0107】関数ACHにより変換RESを計算した後、アクセス・システムSAAは受信要請ランダム・ワ

ードR3を生成し（ステップ108）、変換RES、量C1およびランダム・ワードR3を独立セットPAに送信する（ステップ110）。

【0108】独立セットの側では、DESタイプのアルゴリズムの場合、変換RES'を計算し（ステップ112）、RSAタイプのアルゴリズムの場合には、秘密遠隔ローディング・マスターキーSCHのもとでRESおよびワードRの変換を計算することにより（ステップ114）、システムSAAの署名を実証する。

【0109】システムSAAの認証の場合には、新たなクレジットC2の計算が行なわれる（ステップ116）。

【0110】次いで、前払い手段は、選択された暗号アルゴリズムに応じて、新たなクレジットC2にマスターキーKCHおよびランダム・ワードR3で署名し（ステップ118）、あるいはマスターキーSCHおよびランダム・ワードR3で署名する（ステップ120）。

【0111】最後に、ステップ122において、新たなクレジットC2および変換RES3が送信される。

【0112】アクセス・システムの側では、DESタイプのアルゴリズムの場合はRES3'を計算することにより遠隔ローディングの受け入れの認証を実証し（ステップ126および128）、RSAタイプのアルゴリズムを使用する場合には変換RES3の認証を実証してそれを行なう（ステップ124）。

【0113】遠隔ローディング要請ワードRとその変換RESを交換する前に、遠隔ローディング依頼の認可の認証を得ることを希望して、システム認証手段AUSAおよびAUSAACAが認可認証ワード（ステップ118、図2）およびシステム認証関数KO、SOによるその変換RES1を交換するのは有利である。

【0114】アクセス・システムと認可センターとの間で拒絶が無いことは、一時的遠隔ローディングマスターキーKCHあるいは（PCH、SCH）を用いる原理により保証される。それで、管理当局は、遠隔ローディングの運営に役立つ遠隔ローディング・マスターキーを供給することのできる唯一のものであるため、遠隔ローディングを認可しなければならないのにそれを断るということとはできない。

【0115】他方、アクセス・システムは、遠隔ローディングの認可が遠隔ローディング・マスターキーと結び付けられるときにのみ有効であれば、遠隔ローディングの認可の受け入れを主張することはできない。

【0116】GSMに適用する場合、遠隔ローディング手段ACHPAおよび生成手段AGPAを着脱可能な加入者識別モジュールSIMに収容するのは有利である。

【0117】加入者識別モジュールSIMを利用するGSMの適用において本発明を実行するためには、このモジュールに前払いアプリケーションが存在する必要がある。

【0118】この前払いアプリケーションは非占有の読み取りファイルおよび遠隔ローディング・マスターキー

KCHあるいは(PCH, SCH)を提示することにより更新(アップデート)がプロテクトされている必要がある。

【0119】この遠隔ローディング・マスターキーKCHあるいは(PCH, SCH)は一時的なものであり頻繁にやりとりする当局が、SIMモジュールのメモリに追加されるべきクレジットの価値を提示することにより、前払いファイルに価値を書き込むことを可能にするものである。

【0120】SIMモジュールを使用するGSMアプリケーションでは、無線電話相互通信を確立するための手段MEが、通信している加入者識別モジュールSIMに対し、先述の遠隔ローディングの提案ROを送信し、次いで、一時的遠隔ローディング・マスターキーKCHあるいは(PCH, SCH)により証明された、遠隔ロードされるべき量を含むワードC1を送信する。

【0121】GSMアプリケーションの場合、第一の遠隔ローディング手段および第一の生成手段はSIMモジュールにある。

【0122】モジュールが無線通信運営者により発行される場合、アクセス・システムSAAはVLR(ビタ配置レジスタ VISITOR LOCATION REGISTER)のレベルに配置され、認可センターCAはHLR(ホーム配置レジスタ HOME LOCATION REGISTER)のレベルに配置される。

【0123】交換電話ネットワークのレベルでは、前払いアプリケーションを収容するSIMモジュールは、名目上の配置レジスタに関連する加入者識別番号IMにより識別される。

【0124】通信の間には、SIMモジュールはVLRレジスタのレベルに配置される。

【0125】それで、本発明によれば、SIMモジュールの使用に対する料金の請求を引き受けるのはVLRレジスタである。

【0126】VLRレジスタは任意の時点において残っている前払い手段のクレジットを知っていることに注意すべきである。

【0127】このように、クレジットが所定のしきい値に達すると、レジスタVLRはモジュールSIMに対する遠隔ローディングを提案する際に、モジュールSIMに知らせる。

【0128】この情報に応じて、SIMはランダム数Rを生成し、このランダム数RによりSIMモジュールの能動的な認証が可能になり、図2および図3を参照して説明したように、一時的再ローディング・マスターキーKCHあるいは(PCH, SCH)を生成するように要請する。

【0129】これと同時に、レジスタVLRはレジスタ

HLRとの関係で正当性が確認され、それに対して一時的遠隔ローディング・マスターキーを要請する。

【0130】次にVLRとSIMとの間の遠隔ローディングの実施をチェックするために使用されるのは、この遠隔ローディング・マスターキーである。例としてあげると、ワードR、R0、R1、R2、R3は128ビット長のランダム・ワードとすることができる。遠隔ロードされるべき価値および前払いモジュールで利用できる量C1およびC2は4ビット長である。

【0131】マスターキー・ワードRES0は32ビット長である。

【0132】マスターキー・ワードRES、RES1、RES2およびRES3は128ビット長のワードである。

【0133】マスターキーKOおよびKCは128ビット長のマスターキーであり、遠隔ローディング・マスターキーKCH、(PCHあるいはSCH)は選択される暗号アルゴリズムのタイプに依存して64ビットないし512ビットの範囲で変化することができる。

【0134】本発明は独立セットとアクセス・システムとの間の無線タイプの相互通信に限定されないことに注意されたい。

【0135】実際、本発明は任意の通信ネットワークに関係する。このように、本発明は次のものを用いる装置に適用できる：

—アクセス・システムとの無線連結を備えた移動式あるいは固定式の個人用独立セット；

—アクセス・システムとの有線あるいは無線連結を備えた固定公衆独立セット；

あるいは、

—アクセス・システムとの有線連結を備えた移動式あるいは固定式個人用独立セット。

【0136】このように任意の通信ネットワークに一般的に適用できるということは、本発明の遠隔ローディングのモードが独立セットとアクセス・システムの連結の違いにより影響されないという事実により説明される。

【0137】実際的には、無線電話設備の場合(図1—図4)、独立セットの相互通信モジュールMEはアクセス・システムSAAのベース局BFと会話する無線モジュールである。

【0138】対照的に、有線タイプの電話設備に関しては、独立セットの相互通信モジュールMEは、電話ネットワーク接続装置(例えば、公衆電話接続装置URPあるいはローカルな交換パネル)からなるベース局と会話する有線モジュールである。

【0139】本発明の遠隔ローディング手続きはUPT(Universal Personal Telecommunication)として知られるサービスによく適合することに注目されたい。

【0140】より正確に言えば、そのサービスは、特に各加入者が固有の個人識別番号により知られるという事

実により、そのサービスを提供する幾つかの通信ネットワークを横断して個人的に移動できる可能性を加入者に提供することができる。それで、有線タイプの通信ネットワークにおける移動の際には、加入者は自分の位置をいつでも利用センターに示すことを可能にする登録機能を利用する。

【0141】この結果、図1ないし図4を参照して説明した遠隔ローディング手続きにより、前払いアプリケーションに関してUPTサービスを有利に補充することができる。

【0142】本発明の遠隔ローディング手続きはUPTサービスを持たない有線ネットワークにも適用できることに注目すべきである。例えば、電話カードの文脈で述べれば、第一の運営者により管理されあるいは発行される電話カードにより、第二の運営者により管理される通信ネットワークへアクセスすること、およびその逆を認めるという契約を第一および第二の運営者間で結ぶことができる。

【図面の簡単な説明】

【図1】本発明による無線電話設備を示す略図である。

【図2】本発明による安全な遠隔ローディング手続きの

第一部分を説明するフローチャートである。

【図3】本発明による安全な遠隔ローディング手続きの

第一部分を説明するフローチャートである。

【図4】本発明による遠隔ローディング手続きの第二部分およびその認証を説明するフローチャートである。

【符号の説明】

ACHPA 第一の遠隔ローディング手段

ACHSAA 第二の遠隔ローディング手段

AGPA 第一の生成手段

10 AGCA 第二の生成手段

AUPA 第一のセット認証手段

AUPACA 第二のセット認証手段

AUSAA 第一のシステム認証手段

AUSAACA 第二のシステム認証手段

BF ベース局

CA 認可センター

MG 料金計測手段

MPAY 前払い手段

PA 独立セット

20 RTC 交換電話ネットワーク

SAA アクセス・システム

【図1】

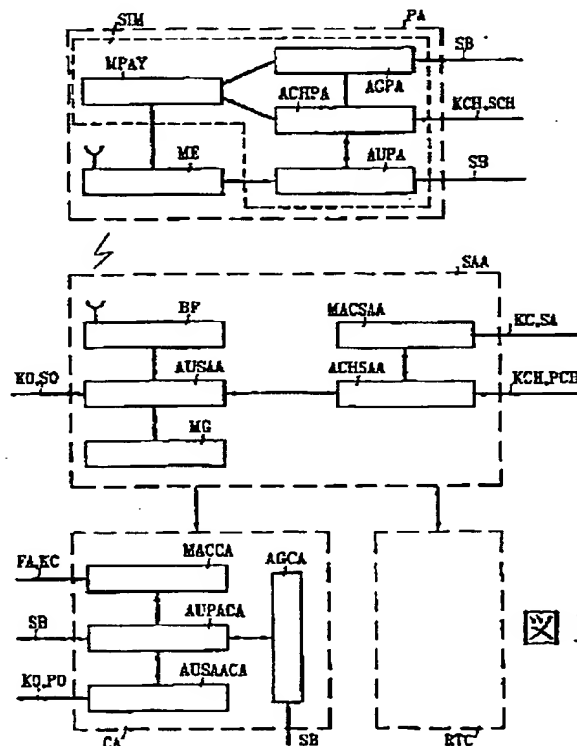


図 1

【図2】

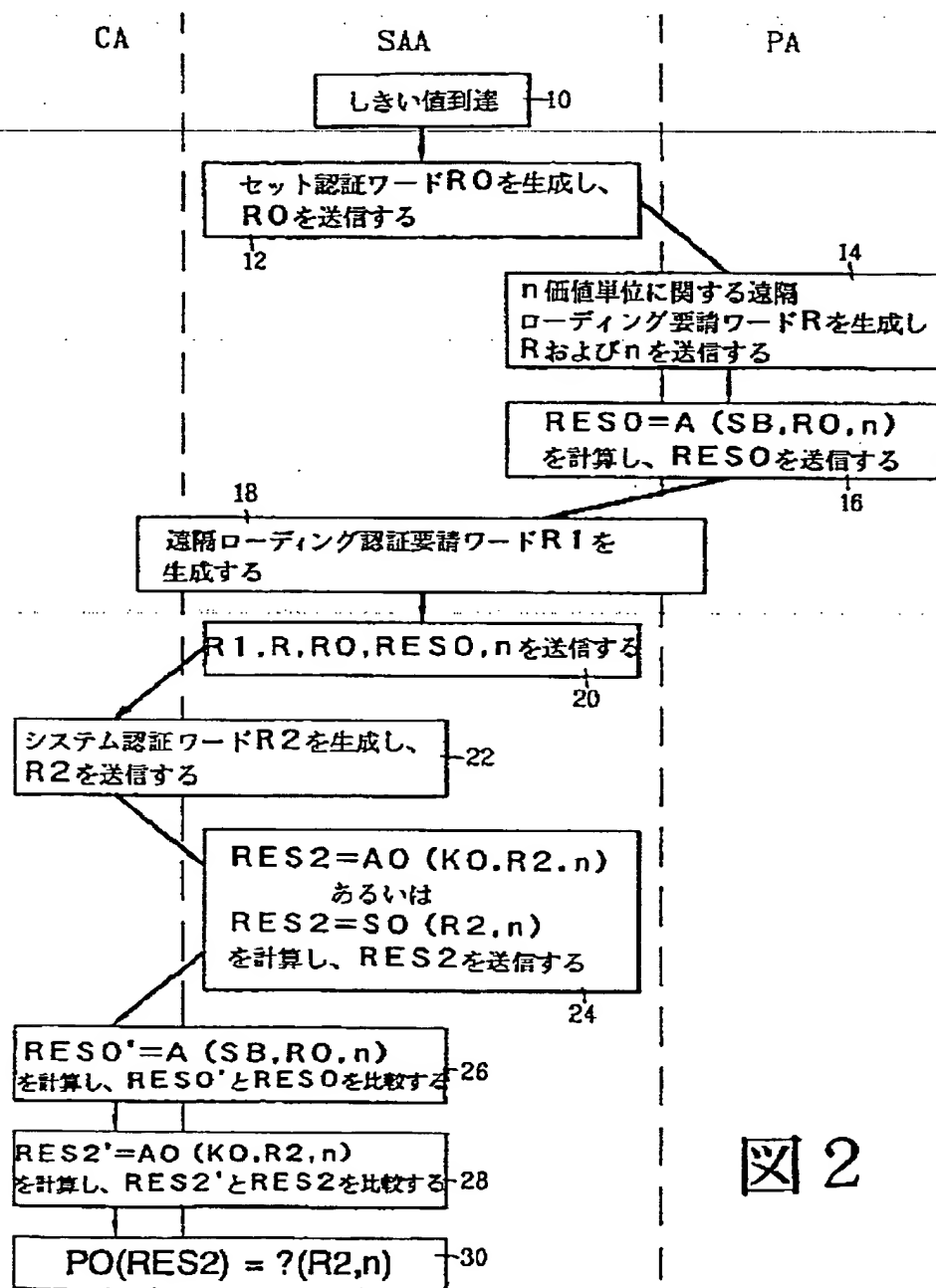


図 2

【図3】

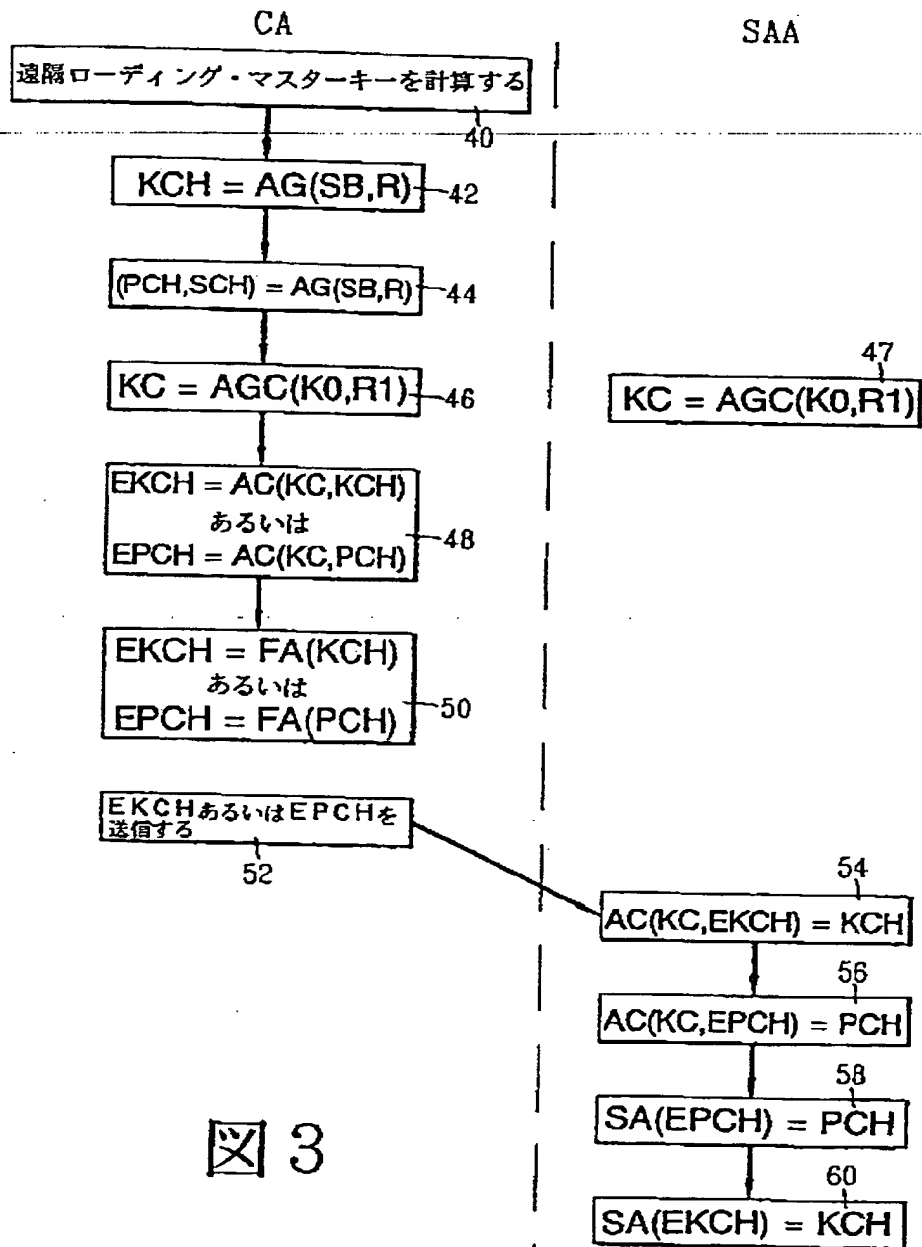


図 3

【図4】

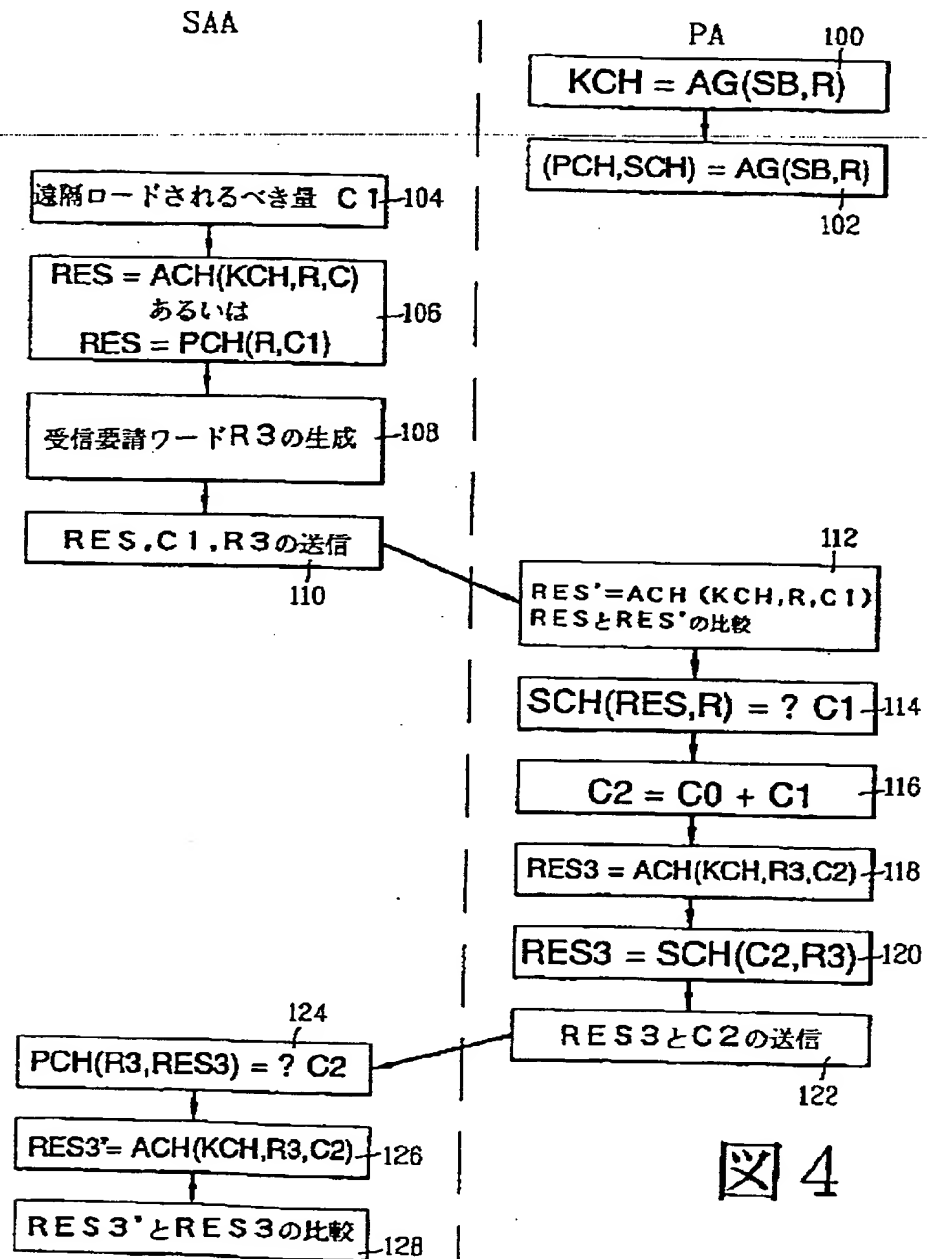


図4

フロントページの続き

(51) Int. Cl. ⁵

9/12

H04Q 7/04

識別記号

庁内整理番号

F I

技術表示箇所

H 7304-5K

7117-5K

H04L 9/00

Z

(72)発明者 ローブ・ヌブ

フランス国、エフ-78990 エランクール

、リュ・ド・モンモランシー、1

(72)発明者 フィリップ・ヨール

フランス国、エフ-14200 エルビーユ・

サン・クレール、グランドデール、1201